

FILED

APR 20 2016


CLERKUNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

16-mj-46

IN THE MATTER OF THE
APPLICATION FOR AUTHORIZATION
TO SEARCH: Six Cellular Phones and
a GPS Device Seized from Christopher
Yellow Eagle, as described in
Attachment A.

**AFFIDAVIT IN SUPPORT
OF APPLICATION FOR
SEARCH WARRANT**

STATE OF SOUTH DAKOTA)
)
COUNTY OF PENNINGTON)

I, Justin M. Hooper, having been sworn, do hereby state as follows:

I am a Special Agent with the Bureau of Indian Affairs (BIA), and have been since April 2010. I am currently assigned to the Division of Drug Enforcement (DDE) in the Rapid City, SD Office. Prior to April 2010, I was employed as a police officer and detective with the City of Flandreau Police Department and as a deputy sheriff in White River, SD with the Mellette County Sheriff's Office. I have six years of road patrol duties which included two years as a part-time narcotics investigator.

During my twelve years in law enforcement, I have participated in investigations of drug offenses. Among other investigative techniques, I have conducted or participated in surveillances, the execution of search warrants, debriefings of informants and reviews of taped conversations. Through my training, education and experience, I have become familiar with the operation of illegal drug trafficking organizations, and the methods used to import and distribute narcotics. Also during my six years with the BIA, I have received

extensive training from experienced BIA special agents and other narcotics investigators in the investigation of drug traffickers.

Based upon my training and experience, including my direct experience in this investigation, I know:

- a) That drug traffickers often maintain, on hand, large amounts of cash (U.S. currency) in order to finance their drug distribution activities;
- b) That it is common for drug traffickers to secrete contraband, proceeds of drug sales, and records of drug transactions in secure locations within their residences, business and vehicles to conceal them from law enforcement.
- c) That drug traffickers commonly maintain addresses or telephone numbers in books, documents and electronic devices that have memory which include computer hard drives, cellular phones, Global Positioning Systems which reflect names, addresses and telephone numbers of the associates in the trafficking organization.
- d) I also know that individuals involved in the distribution of controlled substances and their associates correspond and communicate using internet email, cellular phone text messages and that their computers and/or other electronic storage media in their possession may be used to prepare, create, and maintain writings, records, and documents relating to their activities and associations, including but not limited to the trafficking of controlled substances.

e) Through my own experience and training, I am aware that it is common for narcotics traffickers to utilize cellular telephones to facilitate their drug trafficking activities. I am also aware that in addition to using the telephones for communication purposes, said traffickers may also use the internal memory ("phone book" functions) of the telephone to store names and contact telephone numbers of individuals involved in said drug-trafficking enterprises, and that certain models of cellular telephone also maintain limited logs of past calls made by that telephone.

f) I am also aware that more people, including drug traffickers are utilizing "Smart" phones, such as Apple iPhones, and GPS units for travel directions. These GPS units can be standalone devices manufactured for that single purpose or applications used through cellular phones. Many of the "Smart" phones and GPS units are programmed with addresses from around the United States and all a user has to do is enter the address he/she wants to travel to and the "Smart" phones and GPS units will provide a travel route for the user. Besides providing a travel route for the user most of the "Smart phones" and GPS units also automatically keep track of the route the user has taken and will back track the route to the point of origin.

g) That drug traffickers take or cause to be taken photographs and videos of themselves, their associates, their assets and their product. That these traffickers usually maintain these photographs and videos in their

possession, or within their residences, computers, cellular phones, vehicles, and/or other locations over which they maintain dominion and control;

h) That it is generally a common practice for drug traffickers to maintain in their residences and/or other locations over which they maintain dominion and control records relating to their drug trafficking activities. Because drug traffickers in many instances will "front" (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records (drug ledgers) to show balances due for drugs sold in the past ("pay"), and for payments expected ("owe") as to the trafficker's supplier and the trafficker's dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers, and keep them immediately available in order to efficiently conduct their drug trafficking business. Such records can be maintained on cellular phones.

i) That it is a generally common practice for drug traffickers to make use of wire transfers, cashier's checks, and money orders to pay for expenses associated with services to facilitate their illegal activities. Evidence of such financial transactions and records relating to income and expenditures of money and wealth in connection with drug trafficking would also typically be

maintained in a trafficker's residence and/or other locations over which they maintain dominion and control, including cellular phones.

j) I am also aware that a Subscriber Identity Module ("SIM") card is a portable memory chip predominantly used in cellular phones that hold information regarding the cell phone's number, address, book, text messages, and other data. SIM cards can typically be removed from a phone and placed in another phone, retaining its original data. SIM cards usually have a unique number associated with it so that it can be associated with a particular cell phone service provider.

TECHNICAL TERMS

Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone

numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some

portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

Based on my training, experience, and research I know that the DEVICES have capabilities that allow them to serve as a wireless telephone, a digital camera with photographs and video, and a portable media player of video and music. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICE.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. This information can sometimes be recovered with forensics tools.

Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each of the DEVICES was used, the

purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to

understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

Manner of execution. Because this warrant seeks only permission to examine DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

SCOPE OF REQUEST

I submit this affidavit in support of an application for a warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. 2703(c)(1)(A), authorizing federal law enforcement officers to search the cell phones and

devices found on the person of Christopher Yellow Eagle and in a vehicle being operated by Yellow Eagle, hereinafter identified as the DEVICES, and more fully described and in Attachment "A," and believed to hold evidence of violations of 21 U.S.C. §§ 841(a) and 846.

I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation, from discussions with other law enforcement, from my discussions with witnesses, and from my review of records and reports relating to the investigation. Because this affidavit is being submitted for the limited purpose of securing an order authorizing the search of the DEVICES for the information listed in Attachment B, I have not included details of every aspect of the investigation.

I respectfully submit that probable cause exists to believe that the search of the DEVICES for the information listed in Attachment B will constitute or lead to evidence of offenses involving drug trafficking, particularly violations of 21 U.S.C. §§ 841(a)(1) and 846, hereinafter the TARGET OFFENSES, as well as the identification of individuals who are engaged in the commission of these offenses.

PROBABLE CAUSE

On February 2, 2016, Oglala Sioux Tribe Department of Public Safety (OSTDPS) Officer Alec Morgan Jr. responded to a report of a stolen vehicle. Officer Morgan met with Brian Hill. Hill told Officer Morgan that on January

30, 2016, his estranged wife had loaned their white 2009 Nissan Rogue to her friend, Christopher YELLOW EAGLE, in Rapid City. YELLOW EAGLE took the vehicle and had not returned it yet.

On February 14, 2016, OSTDPS Highway Safety Trooper Ryan Charging Cloud observed a white Nissan Rogue traveling on BIA Hwy 27 on the Pine Ridge Indian Reservation. The vehicle was occupied by a single male driver. The vehicle crossed the center line, the fog line, began driving slower than the posted speed limit, and pulled onto an approach for an unknown purpose. Trooper Charging Cloud recognized that the vehicle matched the description from the stolen-vehicle report. Trooper Charging Cloud initiated a traffic stop of the vehicle and observed the driver making furtive movements in an apparent attempt to hide something under his seat.

Trooper Charging Cloud detained the male who identified himself as Christopher YELLOW EAGLE. Trooper Charging Cloud searched YELLOW EAGLE before placing him in the back of the patrol vehicle. Trooper Charging Cloud located \$985 in US currency inside his right front pant pocket. Trooper Charging Cloud also located a key for room 41 at the Lakota Prairie Ranch Resort. Trooper Charging Cloud asked for consent to search the vehicle and YELLOW EAGLE consented.

Trooper Charging Cloud searched the vehicle, which he noted had the odor of burnt marijuana. In the vehicle Trooper Charging Cloud found: a shell casing for a spent bullet, a partially full box of .45 caliber ammunition, several

small plastic baggies, a glass smoking pipe with what appeared to be methamphetamine residue in it, and two large Ziploc bags containing hundreds of smaller plastic jewelry bags. Trooper Charging Cloud also located a white and black ASUS Zen cellular phone with black duct tape and plastic covering the camera on the phone in the center console of the vehicle. Trooper Charging Cloud also located a black case on the floor board partially under the front seat. Inside of the black case, Trooper Charging Cloud located empty plastic baggies, one of which contained a small amount of a substance that field tested positive for methamphetamine, a digital scale, and hypodermic needle with a small amount of brown colored fluid. The vehicle was towed after the search was completed.

Trooper Charging Cloud called the Lakota Prairie Ranch Resort and spoke with the clerk on duty. Trooper Charging Cloud learned that room 41 was rented to YELLOW EAGLE and that YELLOW EAGLE had paid for the room in cash.

On February 20, 2016, Brian Hill contacted OSTDPS Officer Morgan about some items he found in his Nissan Rogue after he got it back from the police that did not belong to Hill. Specifically, Hill found a black backpack as well as four cellular devices and a black and gray GARMIN "nuvi" GPS device serial number 1TA148417. The four cellular devices are more specifically described as:

- Black ZTE Model Z812 cellular phone with serial number 322452410709

- Black and gray Apple iPhone with a cracked screen and IMEI number 359229060867308
- Black Motorola cellular phone IMEI number: 356378043925395
- Black Samsung Model SCH-RH360 serial number 268435459609208785

Hill contacted police and asked them to take the items. Hill's nephew had downloaded the contents of one of the devices onto an external USB drive which was also provided to law enforcement.

Officer Morgan searched the backpack and located a tan coin purse in the front pocket. The coin purse contained a small amount of loose crystal-like substance that field tested positive for methamphetamine. Officer Morgan contacted SA Justin Hooper after being concerned that some of the items may be part of a mobile methamphetamine laboratory. Officer Morgan took the backpack to the Pine Ridge Justice Center where he met SA Hooper and other agents with the Northern Plains Safe Trails Drug Enforcement Task Force. South Dakota Division of Criminal Investigation (DCI) Special Agent Dane Rasmussen, Federal Bureau of Investigation (FBI) Special Agent Dan Cooper, and SA Hooper searched the backpack. The agents located several items related to the use and distribution of methamphetamine to include, but not limited to, a box of sandwich bags and two small plastic jeweler bags with a blue joker face insignia, a clear plastic canister with a white powder residue, used hypodermic needles with a liquid residue, and unused hypodermic needles. Several miscellaneous receipts and pieces of paper were found in the

backpack including, a Prairie Wind Casino voucher for YELLOW EAGLE and receipts for Jamie Hill.

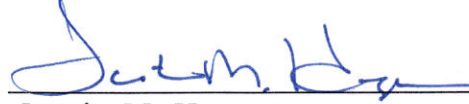
On March 11, 2016, Jackson County Sheriff's Deputy Josh Niesen stopped a vehicle in Jackson County, South Dakota. Melda Terkildsen was the driver, Thomas Thunder Hawk was seated in the front passenger seat and YELLOW EAGLE was in the back seat. Thunder Hawk and YELLOW EAGLE were both arrested on active state warrants. A black Motorola cellular phone with a touch screen, no detachable back, with a rubberized cover and "Verizon" printed on the back, was recovered from the back seat of the car. Terkildsen, Thunder Hawk, and YELLOW EAGLE all denied ownership of the cellular phone.

AUTHORIZATION REQUEST

Based on the foregoing, I respectfully submit there is probable cause to believe that the items listed in Attachment A may contain evidence of offenses in violation of 21 U.S.C. §§ 841(a) and 846, committed by Yellow Eagle.

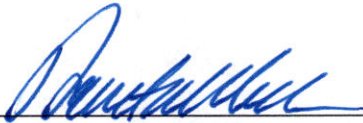
WHEREFORE, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. 2703(c)(1)(A), it is requested that the Court issue a warrant and Order authorizing agents of the BIA and DCI to execute the requested warrant.

Respectfully submitted,



Justin M. Hooper
Special Agent
Bureau of Indian Affairs
Division of Drug Enforcement

Subscribed and sworn to before me this 20th of April, 2016



DANETA WOLLMANN
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF SOUTH DAKOTA